



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|---------------------|------------------|
| 10/058,214 | 01/29/2002 | Robert J. Lambert | 00001-0423 | 2205 |
| 27871 | 7590 | 12/12/2005 | EXAMINER | |
| BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA | | | ABRISHAMKAR, KAVEH | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2131 | |

DATE MAILED: 12/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/058,214

Applicant(s)

LAMBERT ET AL.

Examiner

Kaveh Abrishamkar

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 September 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7 and 9-12 is/are rejected.
- 7) ☒ Claim(s) 8 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment received on September 23, 2005. Claims 1-12 were originally received for consideration. Per the received amendment, claims 1, and 8-10 were amended.

Response to Arguments

2. Applicant's arguments, see Arguments pages 5-9, filed September 23, 2005, with respect to the rejection(s) of claim(s) 1-12 under Kobayashi et al. (U.S. Patent No. 6,430,588) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Kobayashi in view of Schlafly (U.S. Patent No. 5,373,560).

Allowable Subject Matter

3. Claim 8 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kobayashi et al. (U.S. Patent no. 6,430,588) in view Schlafly (U.S. Patent No. 5,373,560).

Regarding claim 1, Kobayashi discloses:

A method of providing a point multiple in an elliptic curve cryptosystem for performing cryptographic operations, said point multiple being derived from a scalar and a point on an elliptic curve having an equation of the form $y^2 + xy = x^3 + ax^2 + 1$, where a is either 0 or 1, said method comprising the steps of:

b) computing a representation of said scalar from said pair of coefficients, said scalar (column 3 lines 25-52, column 11 line 46 – column 12 line 29);

c) computing said point multiple using said representation of said scalar and a Frobenius mapping τ (column 1 line 63 – column 12 line 16, column 11 lines 40-49);

d) providing said point multiple to said elliptic curve cryptosystem for use in said cryptographic operations (column 3 lines 25-52, column 12 lines 26-30).

Kobayashi does not explicitly disclose obtaining a pair of coefficients from a truncator of an elliptic curve. Schlafly discloses a truncation function that takes an input and truncates any other function (the elliptic curve) to discard the fractional part (column 2 lines 60-67). Kobayashi and Schlafly are analogous arts because both pertain to elliptic curve cryptography. It would have been obvious to one of ordinary skill in the art at the time of invention to use the truncation function of Schlafly in conjunction with Kobayashi to save "computation time" (column 1 lines 45-52) when calculating the point multiple.

Claim 2 is rejected as applied above in rejecting claim 1. Kobayashi does not explicitly disclose that the pair of coefficients correspond to an approximation of said inverse. Schlafly discloses that the pair of coefficients can correspond to an inverse (column 2 lines 43-59, column 5 lines 21-45). Kobayashi and Schlafly are analogous arts because both pertain to elliptic curve cryptography. It would have been obvious to one of ordinary skill in the art at the time of invention to use the truncation function of Schlafly in conjunction with Kobayashi to save "computation time" (column 1 lines 45-52) when calculating the point multiple.

Claim 3 is rejected as applied above in rejecting claim 2. Kobayashi does not explicitly disclose the approximation is determined by a significance parameter. Schlafly discloses that the pair of coefficients can correspond to an inverse which is based on a fixed positive constant (significance parameter) (column 2 lines 43-59, column 5 lines 21-45). Kobayashi and Schlafly are analogous arts because both pertain to elliptic

Art Unit: 2131

curve cryptography. It would have been obvious to one of ordinary skill in the art at the time of invention to use the truncation function of Schlafly in conjunction with Kobayashi to save “computation time” (column 1 lines 45-52) when calculating the point multiple.

Claim 4 is rejected as applied above in rejecting claim 1. Kobayashi does not explicitly disclose that the representation of the scalar is equivalent to said scalar modulo said truncator. Schlafly discloses that the representation of the scalar can be modulo of the truncator (column 3 line 50 – column 6 line 2). Kobayashi and Schlafly are analogous arts because both pertain to elliptic curve cryptography. It would have been obvious to one of ordinary skill in the art at the time of invention to use the truncation function of Schlafly in conjunction with Kobayashi to save “computation time” (column 1 lines 45-52) when calculating the point multiple.

Claim 5 is rejected as applied above in rejecting claim 1. Kobayashi does not explicitly disclose computing a quotient derived from said pair of coefficients and said scalar and using said quotient to perform the step of computing said representation of said scalar. Schlafly computing a quotient derived from a pair of coefficients and said scalar and using the quotient to compute the scalar (column 7 line 59 – column 8 line 8).

Kobayashi and Schlafly are analogous arts because both pertain to elliptic curve cryptography. It would have been obvious to one of ordinary skill in the art at the time of invention to use the compute a quotient derived from the coefficients and scalar to compute a representation of the scalar because the quotients and residues will not

exceed the word size of the modulus (column 8 lines 5-8) which would effectively reduce the "computation time" needed (column 1 lines 45-52).

Claim 6 is rejected as applied above in rejecting claim 5. Kobayashi does not explicitly disclose computing a quotient that is equivalent to a product of said scalar and said approximation of said inverse of said truncator. Schlafly discloses computing a quotient a quotient that is equivalent to a product of said scalar and said approximation of said inverse of said truncator (column 7 line 59 – column 8 line 8). Kobayashi and Schlafly are analogous arts because both pertain to elliptic curve cryptography. It would have been obvious to one of ordinary skill in the art at the time of invention to use the compute a quotient that is equivalent to a product of the scalar and the approximation of the inverse of the truncator because it avoids the problem of the residue being longer in words than the modulus (column 7 lines 60-67) which would effectively reduce the "computation time" needed (column 1 lines 45-52).

Claim 7 is rejected as applied above in rejecting claim 6. Kobayashi does not explicitly disclose that the representation of said scalar is equivalent to a remainder after division of said scalar by said truncator. Schlafly computing the representation that is equal to the residue (column 8 lines 8-20). Kobayashi and Schlafly are analogous arts because both pertain to elliptic curve cryptography. It would have been obvious to one of ordinary skill in the art at the time of invention to use a representation of said scalar that is equivalent to a remainder after division of said scalar by said truncator (column 7

lines 60-67) which would effectively reduce the "computation time" needed (column 1 lines 45-52).

Regarding claim 9, Kobayashi discloses:

A method of computing a key for use in a cryptographic system, and said key being derived from a scalar and a point on an elliptic curve having an equation of the form $y^2 + xy = x^3 + ax^2 + 1$, where a is either 0 or 1, said method comprising the steps of:

a) obtaining a pair of coefficients derived from a truncator of said elliptic curve (column 3 lines 25-52, column 6 lines 8-46);

b) computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve (column 3 lines 25-52, column 11 line 46 – column 12 line 29);

c) computing said point multiple using said representation of said scalar and a Frobenius mapping τ (column 1 line 63 – column 2 lines 11, column 11 lines 40-49).

Regarding claim 11, Kobayashi discloses:

In a method of computing an elliptic curve digital signature requiring a point multiple, the improvement comprising computing said point multiple by the steps of:

a) obtaining a pair of coefficients derived from said elliptic curve (column 3 lines 25-52, column 6 lines 8-46);

b) computing a representation of said scalar from said pair of coefficients, said scalar of said elliptic curve (column 3 lines 25-52, column 11 line 46 – column 12 line 29);

c) computing said point multiple using said representation of said scalar and said endomorphism of said elliptic curve (column 1 line 63 – column 2 line 16, column 11 lines 40-49).

Kobayashi does not explicitly disclose obtaining a pair of coefficients from a truncator of an elliptic curve. Schlafly discloses a truncation function that takes an input and truncates any other function (the elliptic curve) to discard the fractional part (column 2 lines 60-67). Kobayashi and Schlafly are analogous arts because both pertain to elliptic curve cryptography. It would have been obvious to one of ordinary skill in the art at the time of invention to use the truncation function of Schlafly in conjunction with Kobayashi to save "computation time" (column 1 lines 45-52) when calculating the point multiple.

5. Claim 11 is a data carrier containing computer executable instructions claim analogous to claim 1, and therefore, is rejected following the same reasoning.

6. Claim 12 is a system claim analogous to the method claim of claim 1, and therefore, is rejected following the same reasoning.


Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
12/07/2005


Primary Examiner
AU 2131
12/8/05